

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE Technical Report		3. DATES COVERED (From - To) -	
4. TITLE AND SUBTITLE Ultra-Dense Quantum Communication Using Integrated Photonic Architecture: First Annual Report			5a. CONTRACT NUMBER W911NF-10-1-0416		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER 0D10BH		
6. AUTHORS Dirk Englund, Karl Berggren, Seth Lloyd, and Gregory Wornell, Chee Wei Wong, Franco Wong, Jeffrey Shapiro			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES Columbia University 615 West 131st Street, Room 254, Mail Code 8725 Studebaker Building New York, NY 10027 -7922				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211				10. SPONSOR/MONITOR'S ACRONYM(S) ARO	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) 58496-PH-DRP.8	
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT The goal of this program is to establish a fundamental information-theoretic understanding of quantum secure communication and to devise a practical, scalable implementation of quantum key distribution protocols in an integrated photonic architecture. We report our progress on experimental and theoretical aspects.					
15. SUBJECT TERMS quantum information, quantum key distribution, photonic integrated chip					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Dirk Englund
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 212-851-5958

## **Report Title**

Ultra-Dense Quantum Communication Using Integrated Photonic Architecture: First Annual Report

### **ABSTRACT**

The goal of this program is to establish a fundamental information-theoretic understand of quantum secure communication and to devise a practical, scalable implementation of quantum key distribution protocols in an integrated photonic architecture. We report our progress on experimental and theoretical aspects.



# Progress on Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

Dirk Englund, Karl Berggren, Seth Lloyd, Jeffrey Shapiro, Chee Wei Wong, Franco Wong, and Gregory Wornell  
(Dated: August 24, 2011)

The goal of this program is to establish a fundamental information-theoretic understand of quantum secure communication and to devise a practical, scalable implementation of quantum key distribution protocols in an integrated photonic architecture. We report our progress on experimental and theoretical aspects.

## Contents

<b>I. Problem Statement</b>	<b>1</b>
<b>II. Information Capacity of a Photon and Transmission in Free Space</b>	<b>1</b>
<b>III. Photonic Integrated Chip</b>	<b>2</b>
<b>IV. Ultrahigh Flux Entangled Photon Source &amp; Time-Energy entanglement d-dimensional QKD</b>	<b>5</b>
<b>V. Self-Differencing Infrared InGaAs Detectors</b>	<b>6</b>
<b>VI. Waveguide-integrated SNSPD</b>	<b>7</b>
<b>VII. Summary of the most important results</b>	<b>11</b>
<b>References</b>	<b>11</b>

## I. PROBLEM STATEMENT

To understand the limits of optical communications, it is necessary to consider light at the level of photons, described by quantum theory. This theory has profound consequences, including the possibility of transmitting information in unconditionally secure ways. However, many questions are still unclear, including the information capacity and transfer rate of optical channels. These questions are of fundamental importance in information science, but are also of increasing technological relevance in emerging communication systems that offer new possibilities in terms of speed, security, and power consumption.

The goal of this program is to experimentally and theoretically investigate the fundamental information capacity of optical communications and to develop revolutionary technology that will enable unprecedented information content, in excess of 10 bits per photon (bpp), while guaranteeing absolute security at high communication rates of 1 Gbps or more. The following sections detail the progress towards theoretical and experimental goals.

## II. INFORMATION CAPACITY OF A PHOTON AND TRANSMISSION IN FREE SPACE

A fundamental question concerns the privacy capacity of optical optical communications, as set by the laws of physics. We are interested in answering this question for the situation in which all degrees of freedom of the photon may be employed, including spatial, temporal, and polarization modes.



We are currently analyzing turbulence-induced cross talk between Hermite-Gaussian modes. Nivedita Chandrasekaran of the J. Shapiro group has worked out turbulence-induced cross-talk behavior between Hermite-Gaussian (HG) modes either with or without the use of adaptive optics at the receiver. She is now in the process of developing similar results for Laguerre-Gaussian (LG) modes, so that we can provide a definitive answer as to whether LG modes offer superior turbulence immunity in comparison with HG modes, as some have speculated. This work is of importance to the quantum communication InPho program because use of a few spatial modes (via hyperentanglement) could ease the equipment requirements for getting to 10 bits/photon at 1 Gbps. We will complete the LG evaluations – and perform the HG versus LG comparisons – in time for the October InPho program review.

The Wornell group is investigating the secrecy capacity of the bosonic wiretap channel. The team has proved a new upper bound on the secrecy capacity of the bosonic wiretap channel. This bound does not rely on any unproven conjecture, including the entropy photon-number inequality. In the low photon-number regime, this upper bound is very close to the capacity expression conjectured in the previous work of Guha, Shapiro, and Erkmen. Moreover the gap in photon efficiency is constant. Encouraged by these results, we are currently investigating the extension to the multi-mode bosonic wiretap channel where, in the low photon-number regime, we anticipate there may be similarly simple capacity bounds.

### III. PHOTONIC INTEGRATED CHIP

The experimental component of this project focuses on the development of an integrated photonic architecture for high-speed, photon-efficient quantum key distribution. The chip will implement the QKD protocol using time-energy entangled photon pairs, which are generated using a spontaneous parametric downconversion (SPDC) source, as discussed below. Alice and Bob have identical chips which contain a photonic integrated circuit (PIC) for the key generation and the security check. An incident photon on Alices or Bobs setup is analyzed either (1) directly on a photon detector or (2) after a Mach Zehnder interferometers that makes up one half of a Franson interferometer, which enables a measurement of the degree of entanglement between the two photons [1]. These measurements corresponds to projections in two bases, (1) and (2). A measurement by Alice reduces the entanglement, which could be detected in the Franson fringe visibility [2]. The optical circuit that implements these measurements is illustrated in Figure 1, in which the ‘X’ symbols represent switches that randomly channel photons between ‘key generation and ‘security check (the two switches in Bobs or Alices setup are synchronized.) The probabilities of performing measurements in the key generation or security check bases can be adjusted dynamically to rapidly adjust the network performance to potentially changing conditions.

In the construction of the photonic integrated chip (PIC), we are currently developing multiple low-loss waveguide couplers, a high-speed on-chip switches, and unbalanced Franson interferometers. Two chip designs have been completed: one employs a single wavelength channel, and the other includes two wavelength channels which are multiplexed and de-multiplexed from the transmission line using chip-integrated add/drop filters. The first test chips are now being fabricated using electron beam lithography. Figure 2 shows an example of an electron beam lithography mask for the photonic networks that will be employed by Alice and Bob.

The chips are designed to implement a quantum key distribution protocol based on reference [2]. Currently, the network is developed with 200-ps long delays, which are visible in the meander patterns, and which enable Alice and Bob to detect an eavesdropper’s POVM with up to 400-ps time duration. The chip also includes sets of two ring-based photonic switches that direct photons to the detector for the generation of the private key, or send them to the Franson interferometer to carry out a security analysis based on the Franson interferometer visibility. The switches combine the outgoing photons onto a common channel, which is then directed to the detectors. In this way, we are able to reduce the number of detectors by factor two compared to the implementation in Reference [2].

The security in the time-bin entangled photon QKD protocol [2] is checked by measuring the visibility of interference fringes in a fourth-order coherence measurement in the Franson interferometer shared between Alice and Bob. In Figure 7, we plot the expected fringe visibility as a function of the time delay in the Franson interferometer arms and as a function of Eve’s POVM timing resolution. The data is plotted for a waveguide loss of 3 dB/cm. To detect Eve’s

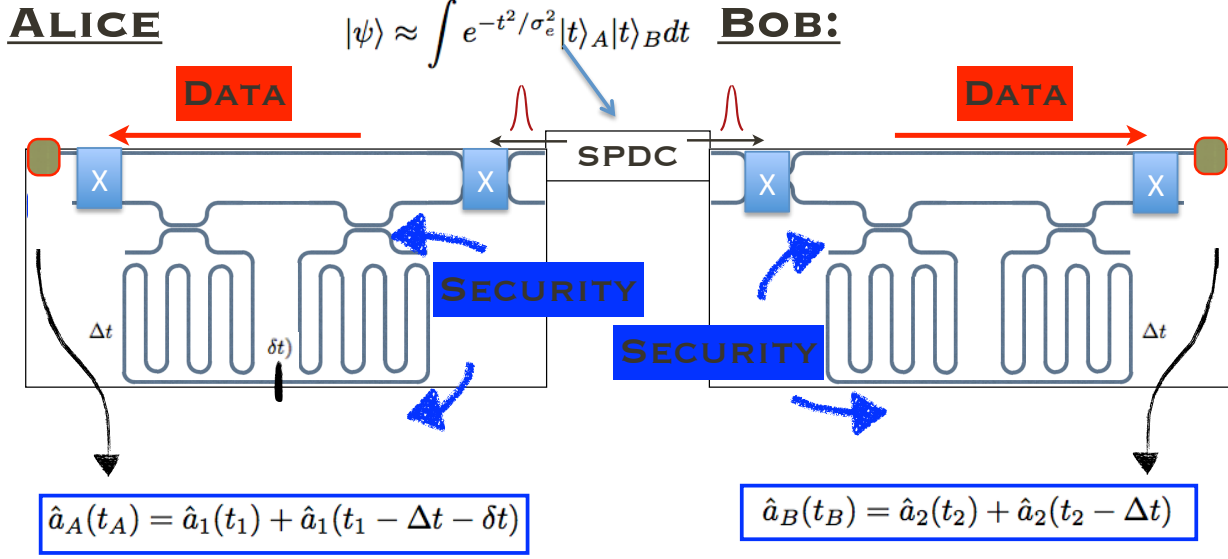


FIG. 1: An entangled photon state is generated by spontaneous parametric down conversion; this is approximated at the biphoton given in the top of the figure. One photon is sent to Alice, the other to Bob. These parties either measure the timing of the photon pair to establish a private key, or they check the security of the protocol using a Franson interferometer. The Franson interferometer employs two unbalanced MZ interferometers with time-difference  $\Delta t$ , enabling coherence measurements to  $2\Delta t$ . A small path difference  $\delta t$  is used to change the coincidence probability from maximum to minimum.

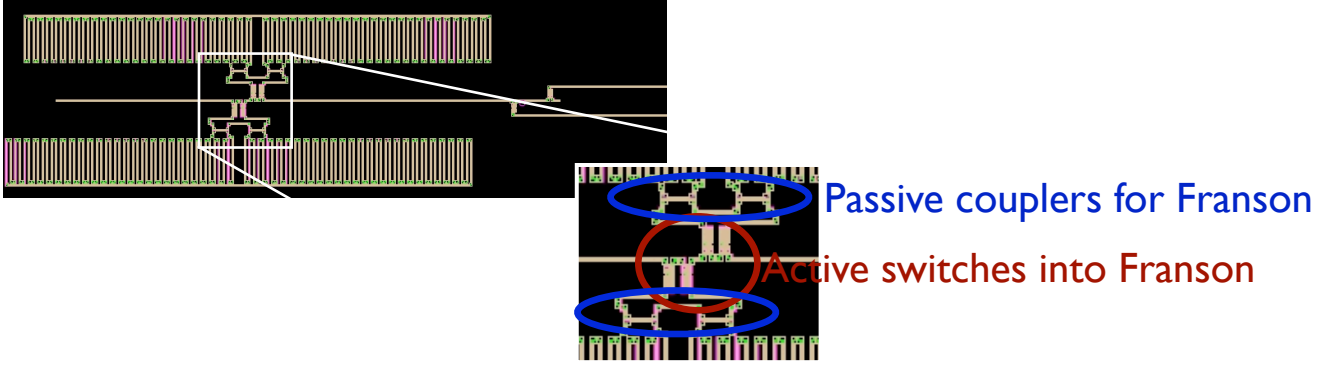


FIG. 2: The mask design shows two wavelength channels (top and bottom arms), each of which includes one half of a Franson interferometer with a 200-ps delay (meander pattern) and two active switches routing light either directly to the detector or first to the interferometer, then the detector.

measurement, the repetition time of the protocol should be below  $\sim 400$  ps. With a detector jitter of 50 ps, this may allow up to eight temporal basis states, though four states is more practical to reduce timing errors. To achieve a larger set of temporal bins, lower waveguide loss will be required. We estimate that most losses are due to surface roughness. We are currently addressing this problem in a two-pronged approach, optimizing the fabrication conditions of the present silicon ridge waveguides, and developing a new waveguide design in which the mode is confined far from the Si surface.

Coupling into and out of the chip is accomplished using inverse-taper waveguide couplers. To scale these couplers to multiple wavelength channels that are anticipated for achieving the targeted bit-rate of 1 Gbit/s, we are currently implementing optical fiber arrays coupled to spatially matched inverse-taper waveguide couplers. Using photonic chips supplied by collaborators at IBM, we have tested the coupling efficiency into and out of a 1-mm silicon-on-insulator

waveguide. Initial experiments indicate total transmission losses below 11 dB. This test required two test setups for Alice and Bob; these are shown in Fig. 3. The system is connected to a new Ti:Sapph laser for the generation of entangled photon pairs by spontaneous parametric down conversion (SPDC). The laser is also used to control the switches using photogenerated carrier injection. Using new high-speed photonic test equipment capable of measuring up to 2 GHz modulation speed, we are currently evaluating the modulation rate and expect to reach over 100 MHz shortly.

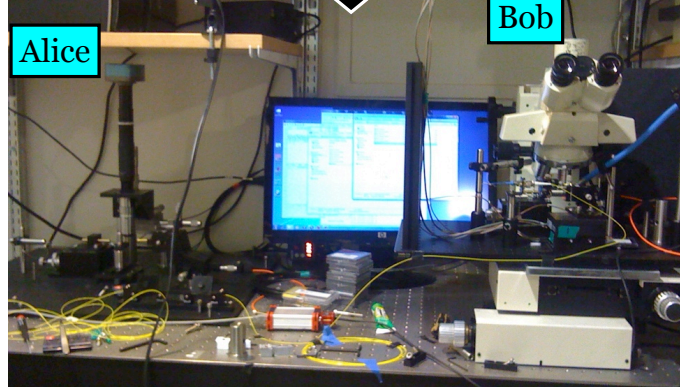


FIG. 3: Optical setups to control the photonic integrated chips for Alice and Bob. The setups contain two 3-axis piezo controlled stages for input/output coupling through inverse tapered silicon waveguides and lensed fibers, as shown on the right. Closed-loop feedback systems controlled from two computers facilitate fiber coupling into and out of the chip; they also lock the maximal alignment for arbitrary times (multiple hours have been tested). The setup also includes a converted high-resolution microscope to control multiple photonic switches by photogenerated carriers.

The chip will furthermore be integrated with the superconducting nanowire single photon detectors (SNSPDs). To this end, we are developing a new technology that we term ‘micro flip-chip bonding’ in which SNSPD detectors, located on a thin sapphire substrate about 20-50 micrometers on the side, are positioned onto matched photonic waveguides on the silicon chip. This technique promises to greatly simplify the integration of superconducting chips with the complex silicon photonic chip architecture. See Section VI for more details.

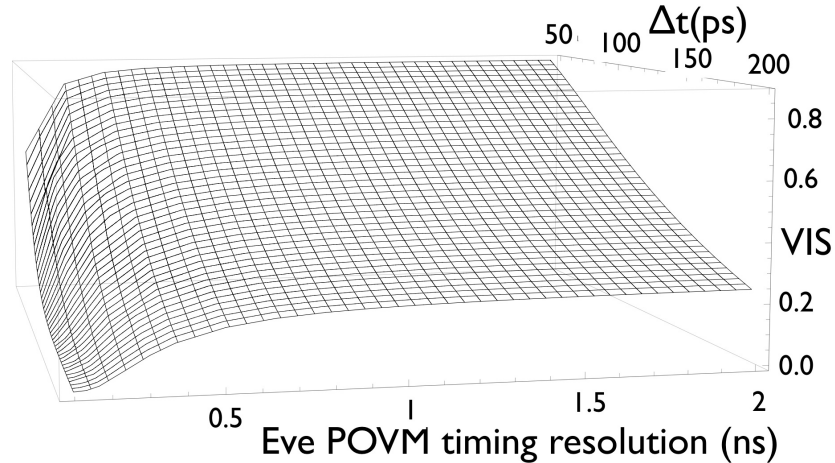


FIG. 4: Mutual information between Alice, Bob, and Eve, as a function of the fraction of time  $\Delta t$ , spent on key generation. The calculation includes the total photon loss and assumes 40 wavelength channels.

**: Mutual information for chip-integrated protocol** We have calculated the mutual information between Alice, Bob, and Eve. The mutual information is calculated from the von Neumann Entropy, assuming that Alice

and Bob spend some fraction of their time,  $\eta$ , on the key generation, rather than the security check. During this time, they measure the visibility of the interference signal on the Franson interferometer; the lower the uncertainty in this measurement, the more they can constrain the amount of information that Eve may acquire. Because of the overhead corresponding to the security check, the key generation rate drops. A full calculation that takes into account photon loss in the entangled photon source, optical fibers, photonic integrated chips, and detectors, implies that 40 wavelength channels are needed to reach a key generation rate of 1Gbps between Alice and Bob. Figure 5 shows mutual information between Alice and Bob (blue), together with Eves information (red). We are currently establishing the privacy amplification protocol to reduce Eves shared information to zero.

mutual information per second, 40 wavelength channels

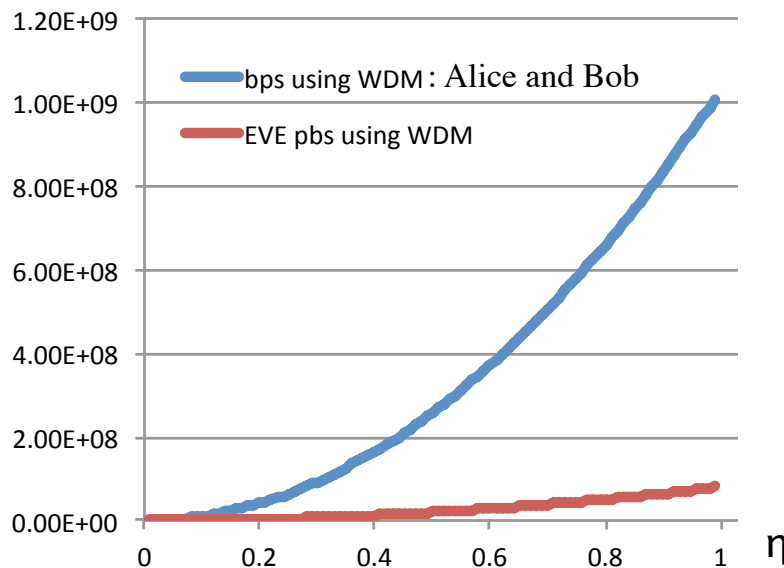


FIG. 5: Mutual information between Alice, Bob, and Eve, as a function of the fraction of time  $\eta$ , spent on key generation. The calculation includes the total photon loss and assumes 40 wavelength channels.

**Metrics:** We have developed fundamental chip components that support the entangled photon QKD protocol. These include the development of high-efficiency waveguides couplers, optical modulators, and low-temperature versions of the photonic integrated chip (PIC). In particular, we have implemented an inverse-taper waveguide coupler design that is scalable to eight channels (waveguides); experimentally we have demonstrate coupling into 1 waveguide and coupling out of 1 waveguide on the same chip, simultaneously. We have measured insertion loss below 3 dB. We have also designed and fabricated the broad-band, high-speed photonic switch required for entangled photon QKD. This chip consists of 3 cascaded rings that, together, provide a square drop filter with 1.2 nm linewidth at 1550 nm; the linewidth is matched to the photon bandwidth.

#### IV. ULTRAHIGH FLUX ENTANGLED PHOTON SOURCE & TIME-ENERGY ENTANGLEMENT D-DIMENSIONAL QKD

The SPDC sources is implemented using PPKTP crystal samples with 46.2  $\mu\text{m}$  grating periods, one from Raicol and one from AdvR, to determine their phase matching curves. We have conducted tests that indicate that nonlinear coefficients and bandwidths are as expected, with Raicol crystal slightly more efficient than AdvR crystal. The phase matching wavelengths for degenerate operation are shifted to the blue of 1560 nm.

In recent months, the group of Franco Wong has started waveguide-SPDC coincidence measurements and assembling a fiber-based Franson interferometer for testing 2-bit time-energy entanglement. For coincidence measurements, the

waveguide was sent to Evaporated Coatings for dual-wavelength AR coating. Recommended by AdvR, the vendor had success in coating waveguides without peeling near the edges of the crystal. The AR coating is expected to be done by the end of August. The necessary single-mode fibers and polarization controllers have been set aside for assembling the fiber-based Franson interferometer. Testing will begin pending the return of the waveguide and completion of the detector assembly. Using single-mode laser inputs at the pump (780 nm) and output (1560 nm) wavelengths, the spatial mode outputs of the waveguide were evaluated, as shown in Fig. 6. We have achieved excellent waveguide-to-fiber coupling efficiency of 75%, 77%, and 80% for pump, signal, and idler, respectively. Signal and idler fields have the same wavelength of 1560 nm but are orthogonally polarized.

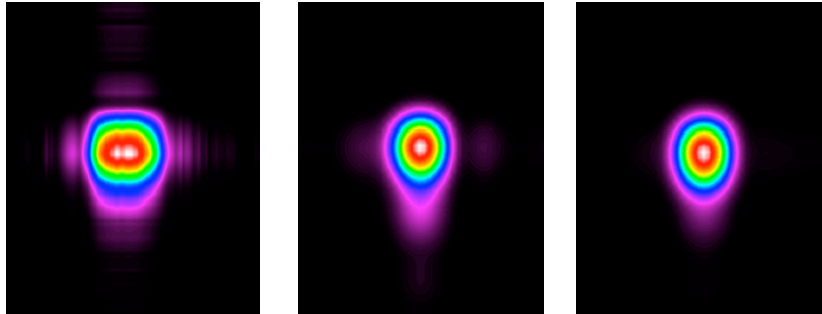


FIG. 6: Measured output mode for pump (left), signal (center), and idler (right).

The Chee Wei Wong group prepared the PPTKP waveguide entangled photon source towards Hong-Ou-Mandel measurements on the chip. All the optical elements for the entangled photon sources are ready, with assistance from MIT; currently we are optimizing the 658.149-nm laser diode for highest entangled photon counts. This is tricky but quite feasible where we have ordered a new laser to pump at higher powers. The new laser will arrive in 3 weeks, and we are likely to complete this preparation in very shortly after.

The Englund group built a new optics setup that employs a PPTKP nonlinear crystal for entangled photon pair generation at 1550 nm. Since we are still setting up the InGaAs single photon detectors, we are testing this setup using difference frequency generation using 1556 nm cw laser and 778 nm cw lasers. The setup will be tested for entangled photon pair generation with the completion of the InGaAs detectors in the coming weeks (see below).

## V. SELF-DIFFERENCING INFRARED INGAAS DETECTORS

While the SNSDPs are still in development, we will employ InGaAs single photon detectors operating in the telecom band. Since InGaAs APDs are typically hampered by a very slow repetition rate of tens of kilohertz, we have begun collaborations with the group of Joshua Biefang at NIST, Gaithersburg, to implement six InGaAs detectors using a novel self-differencing scheme that enables several orders of magnitude higher repetition rate, potentially reaching the GHz regime.

Graduate students Tian Zhong (MIT), Jacob Mower (Columbia), and PI Dirk Englund (Columbia) visited NIST in May and June 2011 to learn about the assembly and testing techniques for the self-differencing circuit board (Fig. 8) develop by Joshua Biefang and collaborators at NIST. MIT built and tested the water-cooled enclosure that also included dry-air circulation to prevent condensation at low temperatures. Columbia has built an air-tight enclosure in which the detectors will be cooled by thermo-electric coolers to a temperature of -40°C. MIT started the second enclosure for the detectors (two detectors per enclosure) to allow operation with 4

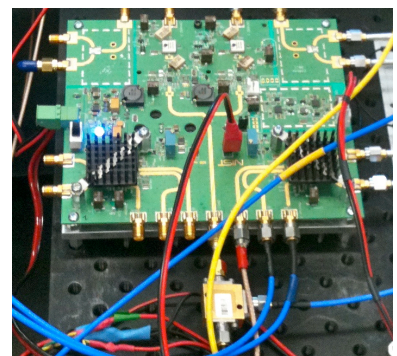


FIG. 8: Self-differencing board for two InGaAs infrared detectors (Columbia/NIST).



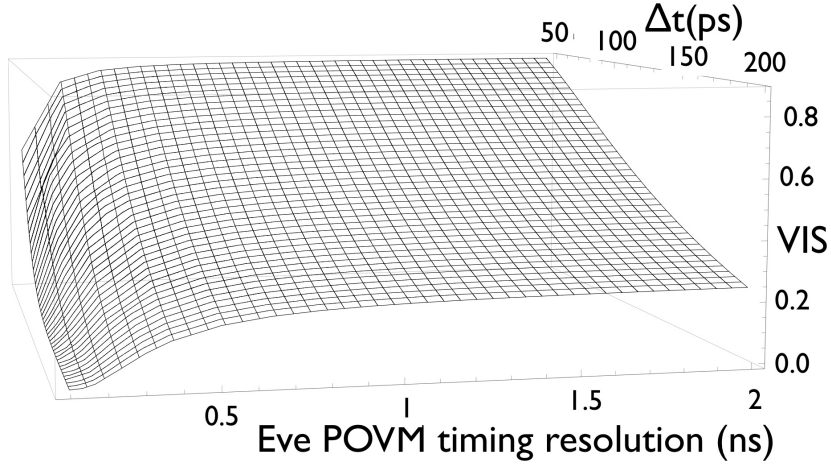


FIG. 7: Visibility as a function of Franson interferometer delay and Eve's POVM timing resolution, assuming 3dB/cm loss in the Si waveguide. Under these conditions,  $\sim 4$  bits (16 bins of 40 ps) appears feasible. For a larger temporal dimension, a lower waveguide loss is being developed.

high-rate detectors. Coincidence measurements will begin pending the return of the waveguide from the coater. The photos in Figure 9 show the top view (left panel) of the detector box containing the electronics and the bottom view (right panel) of the box with the thermoelectric cooling unit.

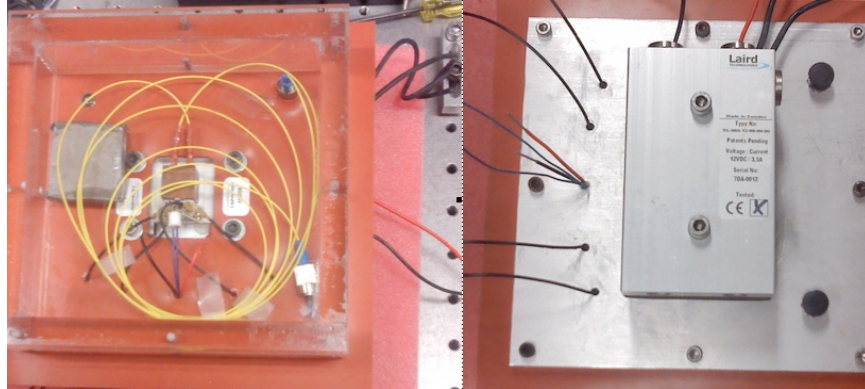


FIG. 9: Water-cooled detector enclosure (MIT/NIST).

## VI. WAVEGUIDE-INTEGRATED SNSPD

The Berggren and Englund groups are presently completing first prototypes of a waveguide (WG)-integrated superconducting nanowire single-photon detector (SNSPD) that will be scalable to eight or more independent detectors. As mentioned above, the integration, which is jointly undertaken by MIT and Columbia, employs a new chip bonding technique that enables optimal absorption of light from a photonic waveguide in Si into the SNSPD.

**Fabrication of an SNSPD on a membrane:** The team's approach to achieving high coupling efficiencies ( $>50\%$ ) between superconducting nanowire single-photon detectors (SNSPDs) and incident light is the integration of these detectors with waveguides. Currently on-chip waveguide systems (based on silicon and other dielectrics) can couple light coming directly from a source (e.g. quantum dot) that is integrated on the same chip. Integrating the entire optical system on a single chip reduces coupling losses and increases system scalability. However, state-of-the-art

SNSPDs are fabricated using NbN films that are grown on bulk Sapphire or MgO wafers. As a result standard detectors are not suitable for integration with an existing on-chip optical system.

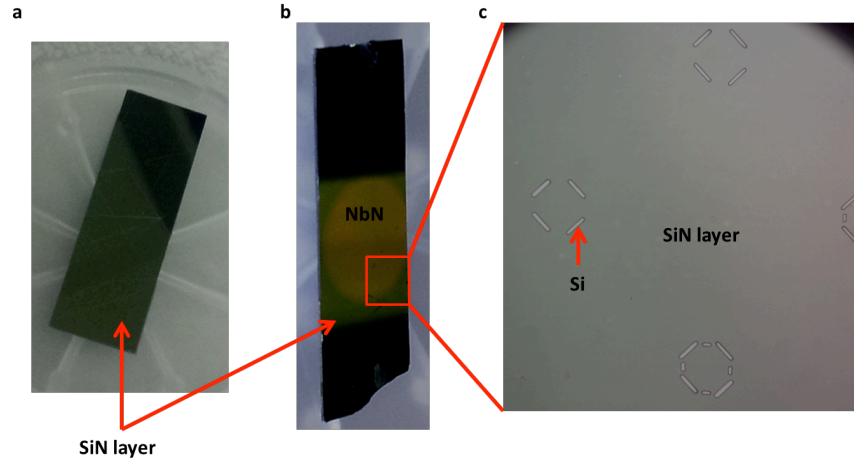


FIG. 10: Silicon Nitride sample for membrane release process. (a) Substrate with 300nm thick SiN grown on top of Silicon. (b) 4nm thick NbN grown on top of SiN. (c) Trenches (tens of microns long) through SiN layer.

SNSPDs are fabricated on a Silicon Nitride (SiN) membrane. A 1 $\mu$ m-thick membrane can be integrated on a chip which includes waveguides, photonic structures or single-photon sources and is thus a very scalable solution. However, the fabrication of SNSPDs on membranes is challenging and has not been demonstrated so far.

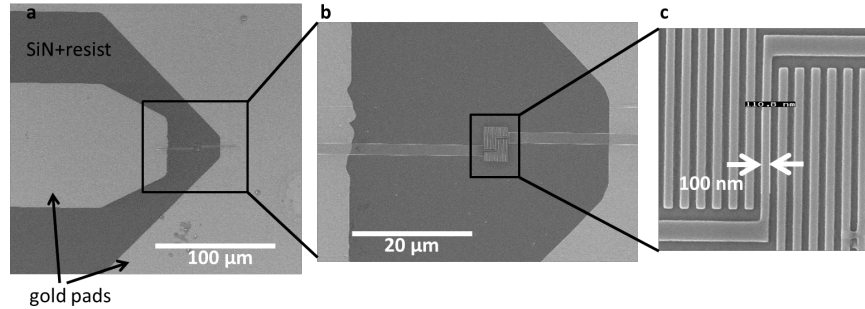


FIG. 11: Nanowires defined in resist on top of gold pads.

Our current fabrication approach is as follows:

1. Processing is done on top of a silicon substrate with a 300nm thick Silicon Nitride (SiN) layer on top (Figure 10(a)). The substrates are provided by MTL at MIT. Status: completed.
2. We grow a 4nm thin Niobium Nitride (NbN) film on top of Silicon Nitride (Figure 10b). We characterized the critical temperature of the NbN films (Figure 12) and obtained 10.6 Kelvin for the best film grown so far, which is suitable for SNSPD fabrication. Status: completed.
3. We define gold pads on top of NbN (Figure 11a). These pads are used as electrical contacts to the SNSPDs. Status: completed.
4. NbN nanowires are fabricated via e-beam lithography (Figure 11c). Status: not completed.
5. We define trenches through the SiN layer (Figure 10c). These trenches are used for a KOH etch process, shown in Figure 14, which only etches silicon. As a result, this process allows us to remove a SiN membrane (with an SNSPD on top) from the substrate. Status: completed.

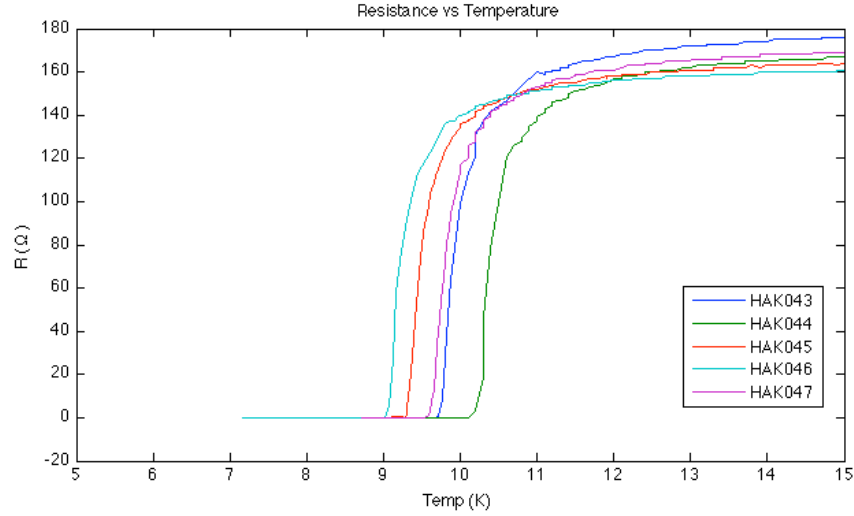


FIG. 12: Film resistance as a function of temperature for different samples. The different curves describe have been grown at different temperatures and Nitrogen pressure values to reach a high critical temperature (TC). The best value obtained was TC=10.6K (green curve).

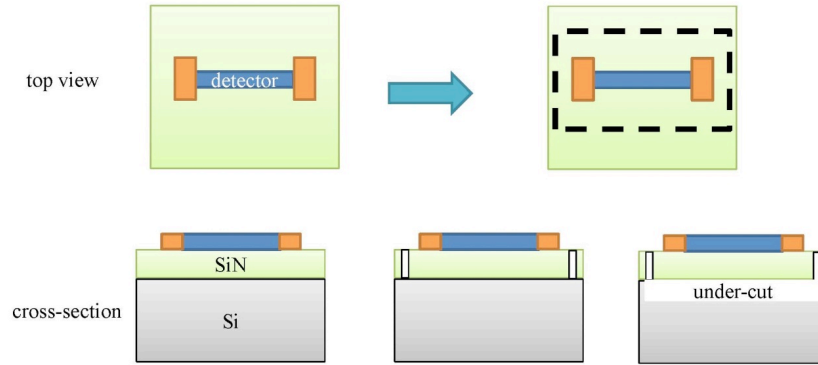


FIG. 13: Fabrication process for SNSPDs on a SiN membrane. Small slits around the detector area are etched through the nitride layer via reactive ion etching. The chip is then dipped into KOH, which selectively etches the Silicon but not Silicon Nitride. This wet-etch process undercuts the thin SiN layer with the detector on top. This small under-cut region can be easily released from the rest of the chip using microscopic probes.

The waveguide (WG) integrated SNSPD will be tested in a dip probe setup, immersed in a liquid He bath ( $T = 4.2$  K). For the characterization the dip probe needs packaging able to exchange optical and electrical signals between the room temperature setup and the cryogenic bath. For the optical part we are going to use a tapered single-mode optical fiber. This will be coupled at room temperature to the waveguide, as shown in Fig. 15. Once the alignment is performed we are going to maintain it by gluing the fiber and waveguide with a UV curable glue.

We will complete the nanowire fabrication process and further optimize the design of the dip-probe setup (already in use for preliminary measurements) which will be used for optical characterization of waveguide-integrated detectors. Integration on Photonic Integrated Chip (Mower and Hoder, Columbia).

We have tested the KOH undercut on SNSPD-on-SiN chips fabricated at MIT. After several iterations between the Columbia and MIT teams, we have been able to etch through the silicon underneath the SiN layer, producing suspended SiN membranes that will be transferred onto the photonic integrated chip (PIC). The KOH etch is anisotropic along Si crystal directions, which can result in slow and un-even etch rates, as shown in Figure 16. To evaluate this, we have



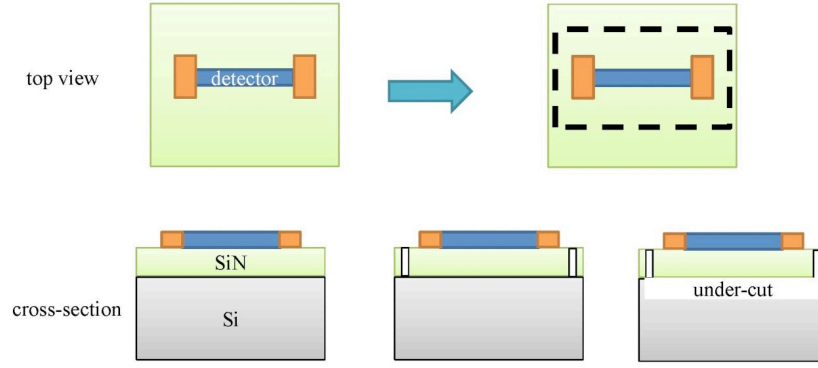


FIG. 14: Single-mode optical fiber aligned to tapered waveguide. The waveguide and the optical fiber are held together by a UV cured glue. Inset. Zoom of the waveguide coupling region cross-section (dark blue); the tip of the optical fiber (light blue) has to be as big as the waveguide coupling region.

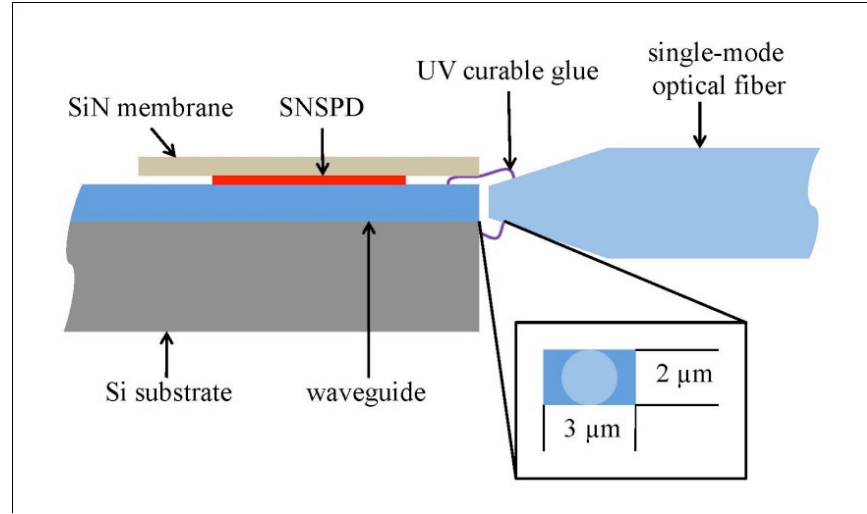


FIG. 15: Dip-probe head which will be used for optical characterization of waveguide-integrated SNSPDs.

adopted a fabrication process in which the trenches are at different rotations with respect to the Si crystal direction, as shown in the Figure. Recently, we have been able to undercut SiN membranes following a longer dry-etch into the Si substrate. An example of a freed membrane is shown in the right panel of Figure 16.

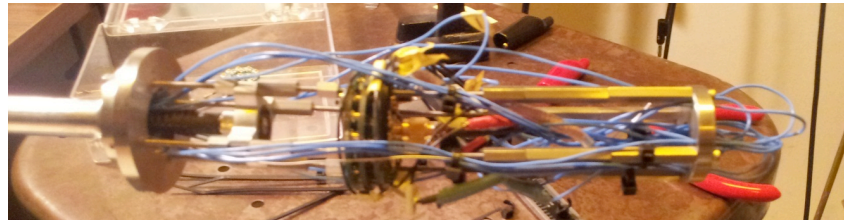


Figure 10: Dip-probe head which will be used for optical characterization of waveguide-integrated SNSPDs.

FIG. 16: SiN membrane pedals and etch tests. Left: rotating the trenches will enable us to evaluate the anisotropic etch rate to improve the process. Center: an unsuccessful etch results in no visible undercut. Right: A successful KOH etch yields suspended SiN membranes.

## VII. SUMMARY OF THE MOST IMPORTANT RESULTS

- We are addressing the question whether LG modes offer superior turbulence immunity in comparison with HG. We have analyzed turbulence-induced cross-talk behavior between Hermite-Gaussian (HG) modes either with or without the use of adaptive optics at the receiver; we are now analyzing Laguerre-Gaussian (LG) modes. This problem is of importance because it dictates how much information may be encoded in spatial degrees of freedom, and with what efficiency this information may be transmitted.
- We proved a new upper bound on the secrecy capacity of the bosonic wiretap channel. This upper bound is very close to the capacity expression conjectured in the previous work of Guha, Shapiro, and Erkmen in the low photon-number regime.
- We have developed designs that will enable photon-efficient quantum key distribution protocols to be implemented on a photonic integrated chip (PIC). The chip design security checks for all degrees of freedom used: time-energy, polarization, and spatial. Security is guaranteed by the laws of physics, not by the technology that Eve may possess.
- We have fabricated the first integrated photonic chips for quantum information processing using photons in the telecommunications band. First tests have been completed with strong lasers, and entangled-photon tests are underway. The chip design implements the program's large-alphabet entangled photon QKD protocol. The chip includes efficient input/output couplers; silicon and silicon nitride waveguides; direct couplers; wavelength division multiplexing (2 channels); and switches, which enable a reduction by a factor of two the number of detectors required, and enable real-time optimization of the QKD security check and key generation.
- We completed two PIC test setups: one for Alice, one for Bob.
- We have developed a process to bring infrared single photon detectors on a photonic integrated chip. In particular, we have completed the first steps of a fabrication technique to bond superconducting nanowire single photon detectors (SNSPDs) on a silicon photonic integrated chip. The chip contains the full network for the QKD protocol. In the future, it may also include electronics for on-chip logic.
- We have implemented a waveguide PPKTP source for spontaneous parametric down conversion in the telecom band (at  $1.55\ \mu\text{m}$ ); we demonstrated waveguide-to-fiber coupling efficiency of 75%, 77%, and 80% for pump, signal, and idler, respectively

- 
- [1] J. D. Franson. Two-photon interferometry over large distances. *Phys. Rev. A*, 44:4552–4555, Oct 1991.
- [2] Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Phys. Rev. Lett.*, 98(6):060503, Feb 2007.